Data Protection Policy

TABLE OF CONTENTS

1 AIMS

Tamworth Self Storage Ltd known herein after as ("The Company") aim to ensure that all personal data collected about staff, clients, directors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) incorporated in to UK data protection law (now called UK GDPR with effect 1 January 2021) under the provisions of the Data Protection Act 2018 (DPA 2018). Any references in this policy to GDPR is now termed as UK GDPR.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2 LEGISLATION AND GUIDANCE

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

In addition, this policy complies with our articles of association.

3 DEFINITIONS

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: Name (including initials) Identification number Location data Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetics Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes Health – physical or mental Sex life or sexual orientation

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Legitimate Interests	Legitimate interests include the following: Compliance with our legal, regulatory and corporate governance obligations and good practice Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests Ensuring business policies are adhered to (such as policies covering email and internet use) Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking Investigating complaints Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments Monitoring staff conduct, disciplinary matters Marketing our business Improving services
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration,

	unauthorised disclosure of, or access to personal data.

4 THE DATA CONTROLLER

Our Company processes personal data relating to service users, staff, directors, visitors and others, and therefore is a data controller.

The Company is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5 ROLES AND RESPONSIBILITIES

This policy applies to **all staff** employed by our Company, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 BOARD OF DIRECTORS

The board of directors has overall responsibility for ensuring that our Company complies with all relevant data protection obligations.

5.2 DATA PROTECTION OFFICER

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Board of Directors and, where relevant, report to the board their advice and recommendations on Company data protection issues.

The DPO is also the first point of contact for individuals whose data the Company processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO Simon Jennings is contactable via email as follows sales@selfstoragetamworth.co.uk or phone on 01827799799.

5.3 CHAIRMAN OR PERSON OF THE BOARD

The Chairman or Person of the Board acts as the representative of the data controller on a day-to-day basis.

5.4 ALL STAFF

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Company of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6 DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that our Company must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes

- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Company aims to comply with these principles.

7 COLLECTING PERSONAL DATA

7.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Company can **fulfil a contract** with the individual, or the individual has asked the Company to take specific steps before entering into a contract
- The data needs to be processed so that the Company can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g., to protect someone's life
- The data needs to be processed so that the Company, can perform a task **in the public interest**, and carry out its official functions or reporting expenditure
- The data needs to be processed for the **legitimate interests** of the Company or a third party (provided the individual's rights and freedoms are not overridden)
- The individual has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 LIMITATION, MINIMISATION AND ACCURACY

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Company's Records Management Policy.

8 SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a member of staff or a visitor that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and service users – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where

we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our contractual obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided
- Processing for payroll, accounts and pension purposes.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9 SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 SUBJECT ACCESS REQUESTS

Individuals have a right to make a 'subject access request' to gain access to personal information that the Company holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

9.2 SUBJECT ACCESS REQUESTS - RECORDS

A record of the Subjects Access Request and the subsequent disclosure will be retained for a period of 12 months and a record of each disclosure will be recorded on the SAR Register.

9.3 RESPONDING TO SUBJECT ACCESS REQUESTS

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Request the Data Subjects permission to disclose the data
- Will respond without delay and within 1 month of receipt of the request
- We may ask the data subject to be specific in relation to the information they require
- Will provide the information free of charge.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of another individual
- Is contained in court order records
- Is given to a court in proceedings concerning the data subject

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 OTHER DATA PROTECTION RIGHTS OF THE INDIVIDUAL

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of a particular lawful basis
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10 PHOTOGRAPHS AND VIDEOS

As part of our Company activities, we may take photographs and record images of individuals within our Company.

We will obtain written consent from employees, clients and visitors, for photographs and videos to be taken for communication, marketing and promotional materials.

We will clearly explain how the photograph and/or video will be used to the employee, visitors or Client. Uses may include:

- Within Company on notice boards and in Company magazines, brochures, newsletters, etc.
- Outside of Company by external agencies such as the Company photographer, newspapers, campaigns
- Online on our Company or subsidiary website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the data subject, to ensure they cannot be identified.

11 DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the Company's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data

protection matters; we will also keep a record of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Company and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

12 DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the DPO
- Passwords that are at least 8 characters long containing letters and numbers are used to access Company computers, laptops and other electronic devices. Staff and directors are reminded to change their passwords at irregular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff or directors who store personal information on their personal devices are expected to follow the same security procedures as for Company-owned equipment.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

NB: Also, see our Records Management Policy.

13 DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Company's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14 EMPLOYEE MONITORING

The Company may from time to time monitor the activities of employee data subjects. Such monitoring may include, but will not necessarily be limited to, internet and email monitoring. In the event that monitoring of any kind is to take place (unless exceptional circumstances, such as the investigation of criminal activity or a matter of equal severity, justify covert monitoring), employee data subjects will be informed of the exact nature of the monitoring in advance.

Monitoring should not (unless exceptional circumstances justify it, as above) interfere with an employee's normal duties.

Monitoring will only take place if the Company considers that it is necessary to achieve the benefit it is intended to achieve. Personal data collected during any such monitoring will only be collected, held, and processed for reasons directly related to

(and necessary for) achieving the intended result and, at all times, in accordance with employee data subjects' rights and the Company's obligations under the GDPR.

The Company shall ensure that there is no unnecessary intrusion upon employee data subjects' personal communications or activities, and under no circumstances will monitoring take place outside of an employee data subject's normal place of work or work hours, unless the employee data subject in question is using Company equipment or other facilities including, but not limited to, Company email, the Company intranet, or a virtual private network ("VPN") service provided by the Company for employee use.

15 PERSONAL DATA BREACHES

The Company will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a Company context may include, but are not limited to:

- A non-anonymised dataset being published on the Company website
- Confidential information being made available to an unauthorised person
- The theft of a Company laptop containing non-encrypted personal data about staff.

Consequences of Failing to Report a Breach

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58, a sample of which are as follows:

a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
e) to order the controller to communicate a personal data breach to the data subject;
f) to impose a temporary or definitive limitation including a ban on processing;

NB: This list is not exhaustive

So, it's important that staff follow the breach-reporting process in place within this policy and to ensure we recognise, detect via our IT provider and can notify a breach, on time; and to provide the necessary details. We shall use the ICO breach reporting form for this purpose as follows https://ico.org.uk/media/for-organisations/documents/2614197/personal-data-breach-report-form-web-20190124.doc .

It is imperative that, where staff feel a breach has occurred, they report this to the DPO at the earliest opportunity.

16 TRAINING

All staff and board members are provided with data protection training as part of their induction process.

17 MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if a fundamental change in legislation occurs, or in any event this policy will be reviewed **every 2 years** and shared with the full Board of Directors.

18 LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- Disciplinary Policy
- Whistle Blowing Policy
- Social Media Policy

- IT Acceptable Use Policy

19 VERSION CONTROL

VERSION	APPROVER	DATE	CHANGES
V.1.0	Simon Jennings	April 2022	First issue

APPENDIX 1 – Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
2. The staff member or data processor will be asked to complete the Company's data breach form at **Appendix 2**.
3. The DPO will assess the nature of the breach and make an initial entry in the Company's breach register.
4. The DPO will inform the Directors of the potential breach
5. On receiving the breach report, the DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
   a) Lost
   b) Stolen
   c) Destroyed
   d) Altered
   e) Disclosed or made available where it should not have been
   f) Made available to unauthorised people
6. The DPO will keep the Directors informed throughout the process
7. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
8. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
9. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g., emotional distress), including through:
   a) Loss of control over their data
   b) Discrimination
   c) Identify theft or fraud
   d) Financial loss
   e) Unauthorised reversal of pseudonymisation (for example, key-coding)
   f) Damage to reputation
   g) Loss of confidentiality
   h) Any other significant economic or social disadvantage to the individual(s) concerned
   i) If it is likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO within 72 hours of the breach being reported.
10. The DPO will document the decision (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are recorded within the Company breach register.
11. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    a) A description of the nature of the personal data breach including, where possible:
       I. The categories and approximate number of individuals concerned
       II. The categories and approximate number of personal data records concerned
    b) The name and contact details of the DPO
    c) A description of the likely consequences of the personal data breach
    d) A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
12. If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

13. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    a) The name and contact details of the DPO
    b) A description of the likely consequences of the personal data breach
    c) A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
14. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    a) Facts and cause
    b) Effects
    c) Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
15. Depending on the severity of the breach, the DPO and Director will either discuss the outcome over the phone or meet to review what happened and how it can be stopped from happening again. This will happen as soon as reasonably possible.

APPENDIX 2 – Internal Breach Report Form

Data Breach Report Form		
This form should be completed as soon as a data breach has been discovered. Please complete sections 1 -7 with as much information as possible and pass the form on to the DPO immediately. The breach will be recorded on the Company's Breach Register and the Directors informed so that an investigation can be carried out		
	Report by:	
	Date	
1	**Nature of breach e.g., theft/disclosed in error/technical problem**	
2	**Description of how breach occurred:**	
3	**When was the breach reported and how did you become aware?**	
4	**Full description of all personal data involved**	
5	**Number of individuals affected?** **Have all individuals affected been informed**	
6	**What immediate remedial action was taken:**	
7	**Has the data been retrieved or deleted? If yes – date and time:**	
8	**Any Procedure changes needed to reduce risks of future data loss**	
9	**Conclusion**	